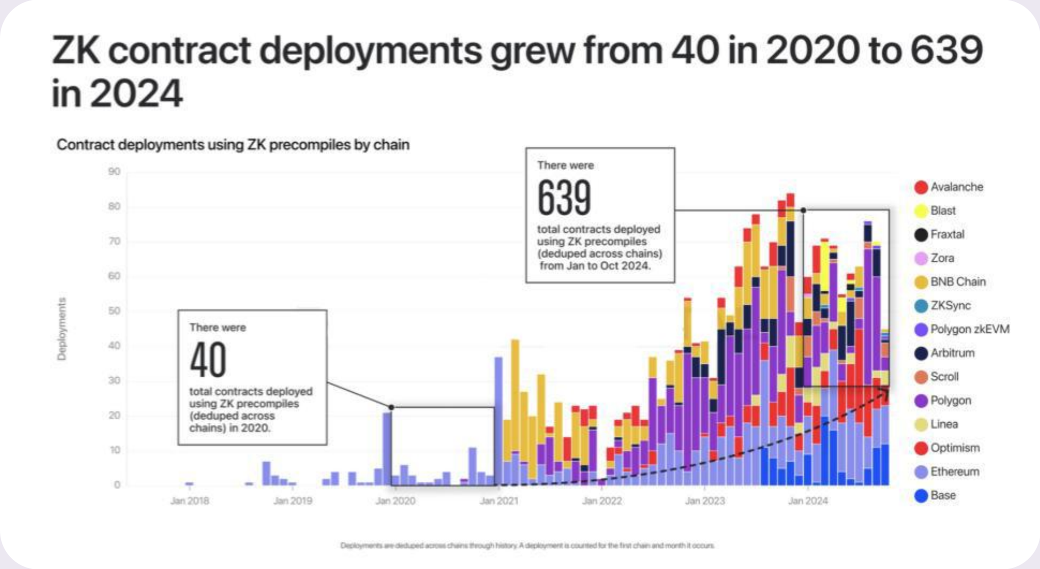
Cardano Budget Proposal

ZK bridge

April 2025

eryx CRYPTO ZK

Don’t Let Cardano Fall Behind in ZK Innovation



ZK contract deployments grew from 40 in 2020 to 639 in 2024

Contract deployments using ZK precompiles by chain

There were 40 total contracts deployed using ZK precompiles (deduped across chains) in 2020.

There were 639 total contracts deployed using ZK precompiles (deduped across chains) from Jan to Oct 2024.

Deployments are deduped across chains through history. A deployment is counted for the first chain and month it occurs.

ZK tech is reshaping blockchain. Other ecosystems are advancing. Cardano risks being left behind.

Cardano Needs Liquidity

No ZK

No bridge

No interoperability

- ☒ No trustless bridge
- ☒ No modular framework
- ☒ No ZK primitives for cross-chain interaction

Our Solution:
A Native zk Bridge for Cardano

A trustless, ZK-powered bridge built in Aiken

Key features:

- ✓ Locking contract on Cardano
- ✓ ZK circuit to prove said locking
- ✓ Minting on target chain
- ✓ Full documentation + open-source

One bridge, two improvements

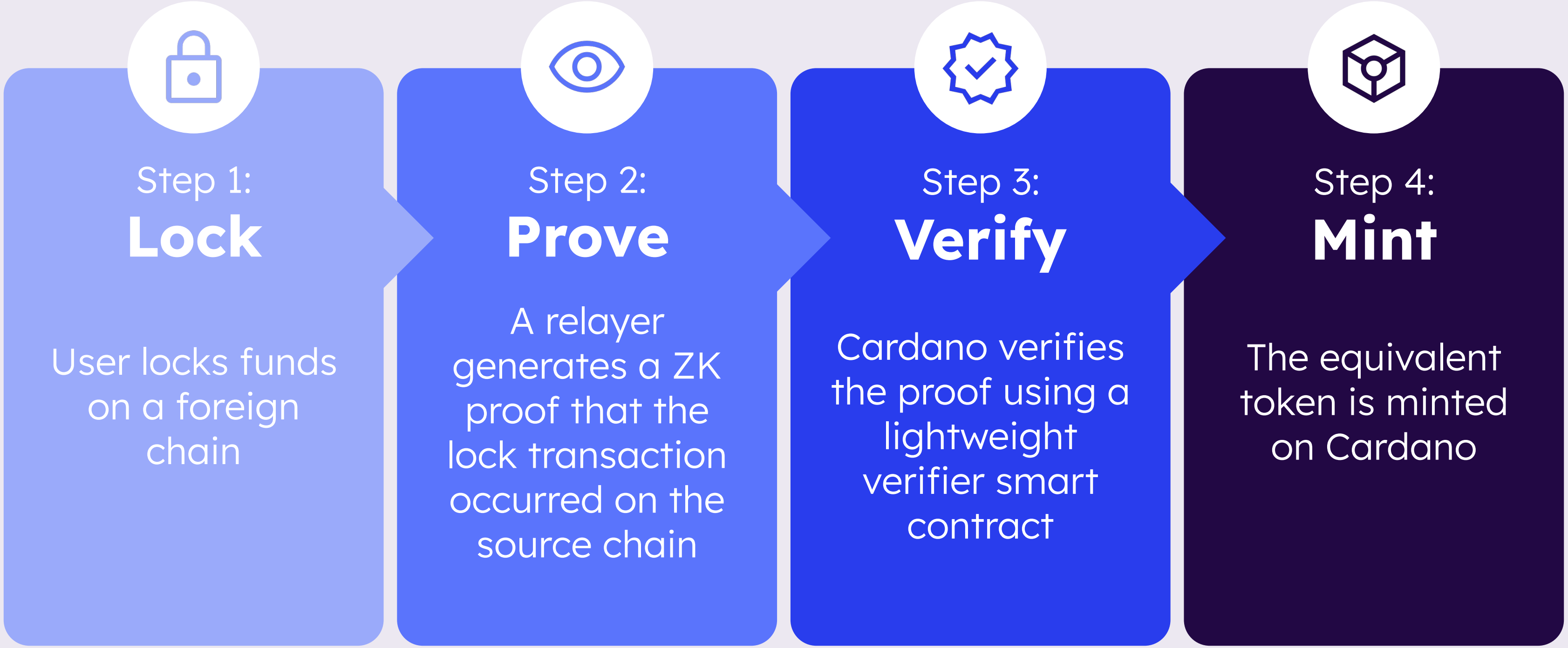
Pillar 1: Zero-Knowledge Foundation

- Extends Zk Cardano ecosystem
- Unlocks future use cases: privacy, identity, zkRollups
- Strengthens the ecosystem with cryptography applications

Pillar 2: Liquidity & Transaction Growth

- Enables trustless bridging with other chains
- Reduces friction for asset flow
- More Liquidity → More use cases → More transactions → Grow the Treasury

How a Zk Bridge works



Step 1:
Lock

User locks funds on a foreign chain

Step 2:
Prove

A relayer generates a ZK proof that the lock transaction occurred on the source chain

Step 3:
Verify

Cardano verifies the proof using a lightweight verifier smart contract

Step 4:
Mint

The equivalent token is minted on Cardano

Open-Source and Mainnet-Ready

100% Open Source

All code, circuits, and documentation will be published publicly under permissive licenses.

Modular & Auditable

Built as standalone components in Aiken, designed for reuse and formal audit.

Mainnet-Ready

Though delivered on testnet, the core implementation is production-grade and can be promoted to mainnet with minimal adjustments.

Developer-Focused

Will include guides, onboarding examples, and tools for easy adoption.

Milestones

1. Documentation of the communication protocol
2. Aiken contracts for locking on Cardano
3. Aiken contracts for minting
4. ZK proof of block inclusion
5. Aiken contract for verifying the ZK proof

Why us?

↓

We are a team of nerds PhDs
with a solid math/cs background, specialized
in blockchain and zero-knowledge
proof cryptography.

Our team

Agustín Garassino

PL and applied ZK cryptographer.

Computer Science M.Sc.

Carlo Giambiagi Ferrari

Applied ZK cryptographer.

Math Phd.

Facundo Decroix

Full stack developer.

Computer Science M.Sc.

Tomás Grosso

Full stack developer.

Computer Science M.Sc.

Caro Lang

Cardano smart contract developer.

Computer Science M.Sc.

Our team

Bruno Weisz

Full stack developer.

Computer Science M.Sc.

Ezequiel Cribioli

Applied ZK cryptographer.

Math M.Sc.

Julián Arnesino

Applied ZK cryptographer.

Computer Science M.Sc.

Agustín Franchella

Advisor. Cardano Ambassador with extensive experience in the ZK and blockchain ecosystem.

Diego Macchi

Business Development and Project Management.

What Have We Been Working On?

Making Cardano ZK Native

zk Proof of Innocence

- Zero-knowledge protocol to prove exclusion from a banned transaction set
- Inspired by privacy-first mechanisms in Ethereum
- Allows a user to prove they did not incur in malicious activity
- ZK circuit built in Circom

API for ZK-SNARK Proof Verification in Aiken

- Infrastructure to verify zk-SNARKs on Cardano
- Demonstrates feasibility of ZK verification on-chain
- Extension of Aiken language to allow for off-chain computing
- Paves the way for future integration of ZK protocols into L1

This **Complements** , Not Competes

Not a rollup. Not a Partner Chain.
This completes the missing layer: interoperability.

Cardano → zkBridge → { Any other chain }

Connects
L1 to the world

Supports
L2 adoption

Enables
Seamless asset flow

Cost Breakdown

Total Requested: $350,000 (≈ 700,000 ADA @ 0.5)

ROLE	USD	ADA
ZK Engineers (2 FTE × 8 mo.)	$180,000	360,000 ADA
Full Stack Engineers (2 FTE × 8 mo.)	$130,000	260,000 ADA
PM / Community / Ops (2 FTE × 8 mo.)	$40,000	80,000 ADA
Total	**$350,000**	**700,000 ADA**

Let’s Build Cardano’s zk Future

zkBridge

Secure

Scalable

Open

Fund the bridge. Unleash Cardano.

eryx CRYPTO ZK